1

GROWTH OF GROUPS AND WREATH PRODUCTS

LAURENT BARTHOLDI

DMA, École Normale Supérieure, 45 rue d'Ulm, 75005 Paris.
Mathematisches Institut, Universität Göttingen, Bunsenstrasse 3-5,
D-37073 Göttingen

To Wolfgang Woess, in fond remembrance of many a visit to Graz

Contents

Introduction

These notes are an expanded version of a mini-course given at Le Louverain, June 24–27, 2014. Its main objective was to gather together useful facts about wreath products, and especially their geometry, in its application to problems and questions about growth of groups. The wreath product is a fundamental construction in group theory, and I hope to help make the reader more familiar with it.

It has proven very useful, in recent years, in better understanding asymptotics of the word growth function on groups, namely the function assigning to $R \in \mathbb{N}$ the number of group elements that may be obtained by multiplying at most R generators. The chapters [4–8] contain many repetitions as well as references to outer literature; by providing a unified treatment of these articles, I may provide the reader with easier access to the results and methods.

I have also attempted to define all notions in their most natural generality, while restricting the statements to the most important or fundamental cases. In this manner, I would like the underlying ideas to

Partially supported by ANR grant ANR-14-ACHN-0018-01 and DFG grant BA4197/6-1.

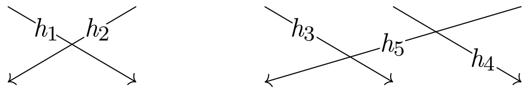
appear more clearly, with fewer details that obscure the line of sight. I avoided as much reference to literature as possible, taking the occasion to reprove some important results along the way.

I have also allowed myself, exceptionally, to cheat. I do so only under three conditions: (1) I clearly mark where there is a cheat; (2) the complete result appears elsewhere for the curious reader; (3) the correct version would be long and uninformative.

I have attempted to make the text suitable for a short course. In doing so, I have included a few exercises, some of which are hopefully stimulating, and a section on open problems. What follows is a brief tour of the highlights of the text.

Wreath Products

The wreath product construction, described in §1, is an essential operation, building a new group W out of a group H and a group G acting on a set X. Assuming[1] that G is a group of permutations of X, the wreath product is the group $W = H \wr_X G$ of H-decorated permutations in G: if elements of G are written in the arrow notation, with elements of X lined in two identical rows above each other and an arrow from each $x \in X$ to its image, then an element of $H \wr_X G$ is an arrow diagram with an element of H attached to each arrow, e.g.



One of the early uses of wreath products is as a classifier for extensions, as discovered by Kaloujnine, see Theorem 1.4: there is a bijective correspondence between group extensions with kernel H and quotient G on the one hand, and appropriate subgroups of the wreath product $H \wr G$, with G seen as a permutation group acting on itself by multiplication. We extend this result to permutational wreath products:

Theorem (Theorem 1.6)**.** *Let G, H be groups, and let G act on the right on a set X. Denote by $\pi : H \wr G \to G$ the natural projection. Then the map $E \mapsto E$ defines a bijection between*

$$\frac{\left\{ \begin{array}{r} E : E \leq H \text{ and the } G\text{-sets } X \text{ and } H\backslash E \text{ are isomorphic} \\ \text{via a homomorphism } E \to G \end{array} \right\}}{\text{isomorphism } E \to E' \text{ of groups intertwining the actions on } H\backslash E \text{ and } H\backslash E'}$$

[1] There is no need to require the action of G on X to be faithful; this is merely a visual aid. See §1 for the complete definition.

and

$$\frac{\left\{\begin{array}{l} E \leq H \wr\wr G : \pi(E) \text{ transitive on } X \text{ and} \\ \qquad \ker(\pi) \cap E \xrightarrow{\cong} H \text{ via } f \mapsto f(x) \text{ for all } x \in X \end{array}\right\}}{\text{conjugacy of subgroups of } H \wr\wr G}.$$

The wreath product $H \wr\wr_X G$ is uncountable, if $H \neq 1$ and X is infinite. It contains some important subgroups: $H \wr_X G$, defined as those decorated permutations in which all but finitely many labels are trivial; and $H \wr_X^{\text{f.v.}} G$, defined as those decorated permutations in which the labels take finitely many different values. Clearly $H \wr_X G \subseteq H \wr_X^{\text{f.v.}} G \subseteq H \wr\wr_X G$, and $H \wr_X G$ is countable as soon as H, G, X are countable.

Growth of Groups

Let us summarise here the main notions; for more details, see §2. A choice of generating set S for a group G gives rise to a graph, the *Cayley graph*: its vertex set is G, and there is an edge from g to gs for each $g \in G$, $s \in S$. The path metric on this graph defines a metric d on G called the *word metric*. The Cayley graph is invariant under left translation, and so is the word metric.

One of the most naive invariants of this graph is its *growth*, namely the function $v_{G,S}(R)$ measuring the cardinality of a ball of radius R in the Cayley graph. If the graph exhibits some kind of regularity, then it should translate into some regularity of the function $v_{G,S}$.

For example, Klarner [47, 48] studied the growth of crystals (that expand according to a precise and simple rule) via what turns out to be the growth of an abelian group.

A convenient tool to study various forms of regularity of a function $v_{G,S}$ is the associated generating function $\Gamma_{G,S}(z) = \sum_{R \in \mathbb{N}}(V_{G,S}(R) - V_{G,S}(R-1))z^R$. The regularity of $v_{G,S}$ translates then into a property of $\Gamma_{G,S}$ such as being a rational, algebraic, D-finite, … function of z.

We may rewrite $\Gamma_{G,S}(z) = \sum_{g \in G} z^{d(1,g)}$; then a richer power series keeps track of more regularity of G:

$$\widehat{\Gamma}_{G,S}(z) = \sum_{g \in G} g z^{d(1,g)}.$$

This is a power series with coefficients in the group ring $\mathbb{Z}G$, and again we may ask whether $\widehat{\Gamma}_{G,S}$ is rational or algebraic[2].

[2] The *rational subring* of $\mathbb{Z}G[[t]]$ is the smallest subring of $\mathbb{Z}G[[t]]$ containing $\mathbb{Z}G[t]$ and closed under Kleene's star operation $A^* = 1 + A + A^2 + \cdots$, for all $A(z)$ with $A(0) = 0$.

The *algebraic subring* of $\mathbb{Z}G[[t]]$ is the set of power series that may be expressed as the solution A_1 of a non-trivial system of non-commutative polynomial equations $\{P_1(A_1, \dots, A_n) = 0, \cdots, P_n(A_1, \dots, A_n) = 0\}$ with coefficients in $\mathbb{Z}G[t]$. The

If G has an abelian subgroup of finite index [52], or if G is word-hyperbolic [33], then $\widehat{\Gamma}_{G,S}$ is a rational function of z for all choices of S. We give a sufficient condition for $\widehat{\Gamma}_{G,S}$ to be algebraic:

Theorem (Theorem 3.2). *Let $H = \langle T\rangle$ be a group such that $\widehat{\Gamma}_{H,T}$ is algebraic, and let F be a free group. Consider $G = H \wr F$, generated by $S = T \cup \{a \text{ basis of } F\}$. Then $\widehat{\Gamma}_{G,S}$ is algebraic.*

We then turn to studying the asymptotics of the growth function $v_{G,S}$. Let us write $v \precsim w$ to mean that $v(R) \le w(CR)$ for some constant $C \in \mathbb{R}_+$ and all $R \ge 0$, and $v \sim w$ to mean $v \precsim w \precsim v$. Then the $\sim$-equivalence class of $v_{G,S}$ is independent of the choice of S, so we may simply talk about v_G.

For 'most' examples of groups, either $v_G(R)$ is bounded by a polynomial in R or $v_G(R)$ is exponential in R. This is, in particular, the case for soluble, linear and word-hyperbolic groups. There exist, however, examples of groups for which $v_G(R)$ admits an intermediate behaviour between polynomial and exponential; they are called groups of *intermediate growth*. The question of their existence was raised by Milnor [58], was answered positively by Grigorchuk [29], and has motivated much group theory in the second half of the twentieth century.

Let $\eta_+ \approx 2.46$ be the positive root of $T^3 - T^2 - 2T - 4$, and set $\alpha = \log 2/\log \eta_+ \approx 0.76$. We shall show that, for *every* sufficiently regular function $f\colon \mathbb{R}_+ \to \mathbb{R}_+$ with $\exp(R^\alpha) \precsim f \precsim \exp(R)$, there exists a group with growth function equivalent to f:

Theorem (Theorem 6.2). *Let $f\colon \mathbb{R}_+ \to \mathbb{R}_+$ be a function satisfying*

$$f(2R) \le f(R)^2 \le f(\eta_+ R) \text{ for all } R \text{ large enough.}$$

Then there exists a group G such that $v_G \sim f$.

Thus, groups of intermediate growth abound, and the space of asymptotic growth functions of groups is as rich as the space of functions. Furthermore, we shall show that there is essentially no restriction on the subgroup structure of groups of intermediate growth. Let us call a group H *locally of subexponential growth* if every finitely generated subgroup of H has growth function $\precnsim \exp(R)$. Clearly, if H is a subgroup of a group of intermediate growth then it has locally subexponential growth. We show, conversely:

Theorem (Theorem 7.1). *Let B be a countable group locally of subexponential growth. Then there exists a finitely generated group of subexponential growth in which B imbeds as a subgroup.*

solution is actually rational if furthermore the P_i are of the form $c_{i,0}+\sum_{j=1}^n c_{i,j} A_j$ with $c_{i,j} \in \mathbb{Z}G[t]$.

Finally, it may happen that a group G has exponential growth, namely that the growth rate $\lim_{R\to\infty} v_{G,S}(R)^{1/R}$ is >1 for all S, but that the infimum of these growth rates, over all S, is 1. Such a group is called of *non-uniform exponential growth*. The question of their existence was raised by Gromov [35, Remarque 5.12]. Again, soluble, linear and word-hyperbolic groups cannot have non-uniform exponential growth; but, again, it turns out that such groups abound. We shall show:

Theorem (Theorem 8.2)**.** *Every countable group may be imbedded in a group of non-uniform exponential growth.*

Furthermore, the group W in which the countable group imbeds may be required to have the following property: there is a constant K such that, for all $R>0$, there exists a generating set S of W with

$$v_{W,S}(r) \leq \exp(Kr^\alpha) \text{ for all } r \in [0, R].$$

(Self-)Similar Groups and Branched Groups

All the constructions mentioned in the previous subsection take place in the universe of *(self-)similar groups*. Here is a brief description of these groups; see §4 for details.

Just as a self-similar set, in geometry, is a set describable in terms of smaller copies of itself, a *self-similar group* is a group describable in terms of 'smaller' copies of itself. A *self-similar structure* on a group G is a homomorphism $\phi\colon G \to G \wr_X P$ for a permutation group P of X. Thus, elements of G may be recursively written in terms of G-decorated permutations of X. For this description to be useful, of course, the homomorphism ϕ must satisfy some non-degeneracy condition (in particular be injective), and P should be manageable, say finite.

The fact that the copies of G in $G \wr_X P$ are 'smaller' than the original is expressed as follows: there is a norm on G such that, for $g \in G$ and $\phi(g)$ a permutation with labels $(g_x : x \in X)$, the elements g_x are shorter than g, at least as soon as g is long enough. For example, consider G finitely generated, and denote by $\|\cdot\|$ the word norm on G. One requires $\|g_x\| < \|g\|$ for all $x \in X$ and all $\|g\| \gg 1$; this is equivalent to the existence of $\lambda \in (0,1)$ and $K \geq 0$ such that $\|g_x\| \leq \lambda\|g\| + K$ for all $x \in X, g \in G$.

Furthermore, in cases that interest us, the map ϕ is almost an isomorphism, in that its image $\phi(G)$ has finite index in $G \wr_X P$. Thus, ϕ may be thought of as a *virtual isomorphism* between G and G^X, namely an isomorphism between finite-index subgroups. When one endows G^X with the ℓ^∞ metric $\|(g_x)\| = \max_{x\in X}\|g_x\|$, the aforementioned condition requires that this virtual isomorphism be a contraction. On the other hand, endowing G^X with the ℓ^1 metric $\|(g_x)\| = \sum_{x\in X}\|g_x\|$, the optimal Lipschitz constant of the virtual isomorphism plays a fundamental role in estimating the growth of G.

Similar groups are a natural generalization: one is given a set Ω and a self-map $\sigma : \Omega \circlearrowleft$; for each $\omega \in \Omega$, a group G_ω and a permutation group P_ω of a set X_ω; and homomorphisms $\phi_\omega\colon G_\omega \to G_{\sigma\omega} \wr_{X_\omega} P_\omega$. Taking for Ω a singleton recovers the notion of a self-similar group. Taking $\Omega = \mathbb{N}$ and $\sigma(n) = n + 1$ defines in full generality a similar group G_0; but it is often more convenient to consider a larger family of groups in which $(G_n)_{n\in\mathbb{N}}$ imbeds. In particular, one obtains a *topological space* of groups, in such a manner that close groups have close properties (for example, their Cayley graphs coincide on a large ball).

Acknowledgments

I am very grateful to Yago Antolin, Laura Ciobanu and Alexey Talambutsa for having organised the workshop in Le Louverain where I presented a preliminary version of this text, and to the participants of the workshop for their perspicacious questions.

A large part of the material is taken from articles written in collaboration with Anna Erschler, and I am greatly indebted to her for generously including me on her projects. It owes much to her energy and enthusiasm that we were able to finish our joint articles.

Hao Chen, Yves de Cornulier and Pierre de la Harpe helped improve these notes by pointing out a number of mistakes and inconsistencies.

Open Problems

This text presents a snapshot of what is known about growth of groups in 2014; a large number of open problems remain. Here are some promising directions for further research.

1. Which groups G are such that, for all generating sets S, the complete growth series $\widehat{\Gamma}_{G,S}$ is a rational function of z?

   This is known to hold for virtually abelian groups, and for word-hyperbolic groups. Conjecturally, this holds for no other group.

   The related question of which groups have a rational (classical) growth function is probably more complicated, see §2.1.
2. Is the analytic continuation $1/\widehat{\Gamma}_{G,S}(1)$ related to the complete Euler characteristic of G, just as $1/\Gamma_{G,S}(1)$ is (under some additional conditions) the Euler characteristic of G? See [74, §1.8] for complete Euler characteristic.
3. Does there exist a group G with two generating sets S_1, S_2 such that $\widehat{\Gamma}_{G,S_1}$ is rational but $\widehat{\Gamma}_{G,S_2}$ is transcendental?

   Such an example could be $G = F_2 \times F_2$. Set $S = \{x, y\}^{\pm 1}$ a free generating set of F_2, and $S_1 = S \times \{1\} \sqcup \{1\} \times S$ and $S_2 = S_1 \sqcup \{(s, s) : s \in S\}$.

   The same properties probably hold for the usual generating series Γ_{G,S_1} and Γ_{G,S_2}. The radius of convergence of Γ_{G,S_1} is 1/3, but that of Γ_{G,S_2} is unknown.

This problem is strongly related to the 'Matching subsequence problem', which asks for the longest length of a common subsequence among two independently and uniformly chosen words of length n over a k-letter alphabet; see [16]. It is easy to see that, for two uniformly random reduced words of length n in F_2, the longest common subword has length $\approx \gamma n$ for some constant γ, as $n \to \infty$. Thus, a pair $(g, h) \in G$ with $\|g\| = \|h\| = n$ has length $2n$ with respect to S_1, but approximately $(2 - \alpha)n$ with respect to S_2. We might call γ the *Chvátal-Sankoff constant* of F_2.

4. Are there infinite simple groups of subexponential growth?[3]

   There is no reason for such groups *not* to exist; but the construction methods described in this text yield groups acting on rooted trees, which therefore are as far as possible from being simple.

   There is also no reason for finitely presented groups of subexponential growth *not* to exist; again, the obstacle is probably more our mathematical limitations than fundamental mathematical reasons.

   The following question, by de la Harpe [38], is still open at the time of writing: 'Do there exist groups with Kazhdan's property (T) and non-uniform exponential growth?'

   Similarly, it is not known whether there are simple finitely generated groups of non-uniform exponential growth, and whether there are finitely presented groups of non-uniform exponential growth.

5. Are there groups whose growth function lies strictly between polynomials and $\exp(R^{1/2})$?

   See the discussion in §2.3. There is a superpolynomial function $f(R) \succsim R^{(\log R)^{1/100}}$ such that no group has growth strictly between polynomials and $f(R)$. There is no residually nilpotent group whose growth is strictly between polynomials and $\exp(R^{1/2})$, see Theorem 5.2.

6. What is the asymptotic growth of the first Grigorchuk group? What is its exact growth, for the generating set $\{a, b, c, d\}$? Does the growth series of the Grigorchuk group exhibit some kind of regularity?

   Some experiments indicate that this must be the case. For example, consider the quotient G_n of the first Grigorchuk group that acts on $\{\mathbf{0}, \mathbf{1}\}^n$. It is a finite group of cardinality $2^{5 \cdot 2^{n-3}+2}$. For $n \leq 7$, the diameter D_n of its Cayley graph (for the natural generating set $\{a, b, c, d\}$) is the sequence $1, 4, 8, 24, 56, 136, 344$ and satisfies the recurrence $D_n = D_{n-1} + 2D_{n-2} + 4D_{n-3}$. If this pattern went on, the growth of the first Grigorchuk group would be asymptotically $\exp(R^{\log 2/ \log \eta_+}) \approx \exp(R^{0.76})$.

[3] This question has been answered positively by V. Nekrashevych, see https://arxiv.org/abs/1601.01033.

If a group has subexponential growth, then its growth series is either rational or transcendental, and if the group has intermediate growth, then the growth series must be transcendental; See Theorem 2.1 in §2.1. Thus, Grigorchuk group's growth series is transcendental. Does the series satisfy a functional equation? That would make it akin to the classical partition function $\sum_{n\geq 0} p(n)z^n = \prod_{n\geq 1}(1 - z^n)^{-1}$, which (up to scaling and multiplying by $z^{1/24}$) is a *modular function*.[4] Ghys asked me once: 'Is the growth series $\Gamma(z)$ of Grigorchuk's group modular?'

7. For every $k \in \mathbb{N}$, the *space of marked k-generated groups* $\mathscr{S}_k$ may be defined as the space of normal subgroups of the free group F_k, by identifying $G = \langle s_1, \dots, s_k\rangle$ with the kernel of the natural map $F_k \to G$ sending generator to generator. It is a compact space. What properties does the set $\mathscr{I}$ of groups of intermediate growth, and the set $\mathscr{N}$ of groups of non-uniform exponential growth, enjoy in this space? For example,

   'Is there an uncountable open subset of $\mathscr{S}_k$ in which $\mathscr{N}$, or $\mathscr{I}$, is dense? Is $\mathscr{N}$ dense in the complement of groups of polynomial growth?'

   Recall that similar groups are families of groups $(G_\omega)_{\omega\in\Omega}$ indexed by a space Ω. If all G_ω are k-generated, we obtain a map $\Omega \to \mathscr{S}_k$, which under favourable circumstances is continuous. This has been exploited, for example, in [60] to produce groups of non-uniform exponential growth.

   It had actually been doubted, before Grigorchuk's discovery [29], whether there were groups of intermediate growth. This text tries to convince the reader that they are abundant. Giving a precise meaning to the above question would quantify, in some manner, the extent to which they are abundant.

Notational Conventions

I try to adhere to standard group-theoretical notation. In particular, the right action of a group element g on a point x is written xg, and a left action is written ${}^g x$. The stabilizer of x is written G_x. The conjugation action of a group on itself is written $g^h = h^{-1}gh$, and the commutator of two elements is $[g, h] = g^{-1}h^{-1}gh = g^{-1}g^h = h^{-g}h$.

I also introduce a minimal amount of new, 'fancy' notation to represent elements of wreath products or of self-similar groups, and hope that it helps in achieving clarity and conciseness.

[4] I.e. a function $A(z) = A(\exp(2\pi i\tau))$ such that the corresponding function $\tau \mapsto A(\exp(2\pi i\tau))$ on the upper half plane is invariant under a finite-index subgroup of $SL_2(\mathbb{Z})$.

1. Wreath Products

We start with the basic construction. Let H be a group, and let G be a group acting on the right on a set X. We construct two groups:

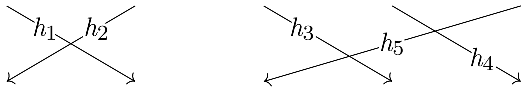
$$H \wr_X G = \Big(\prod_X{}' H\Big) \rtimes G \qquad \text{the \emph{restricted} wreath product,}$$

$$H \wr\wr_X G = \Big(\prod_X H\Big) \rtimes G \qquad \text{the \emph{unrestricted} wreath product.}$$

Here the unrestricted product $\prod_X H$ may be viewed as the group of functions $X \to H$, with pointwise composition and with left G-action given by pre-composition[5]: ${}^g f$ is the function given by $({}^g f)(x) = f(xg)$. The *restricted* product $\prod'_X H$ is then identified with finitely supported functions $X \to H$. In both cases, this product is a subgroup of the wreath product and is called its *base group*.

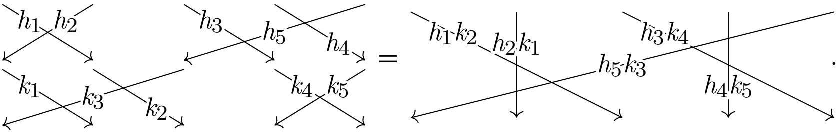
In the particular case of $X = G$ with natural right action by multiplication, one calls $H \wr\wr_G G$ the *regular unrestricted wreath product* and writes it simply $H \wr\wr G$; and similarly for the *regular restricted wreath product* $H \wr_G G = H \wr G$.

Assume that the action of G on X is faithful; so that elements of G may be identified with permutations of X. The best way to describe elements of $H \wr\wr_X G$ or its subgroup $H \wr_X G$ is by *decorated permutations*: one writes a permutation of X, decorated by elements of H, such as



(1.1)

Permutations are multiplied as usual: by stacking them and pulling the arrows tight. Likewise, decorated permutations are multiplied by stacking them and multiplying the labels along the composed arrows. We do not write the labels when they are the identity. Here is a graphical computation of a product:



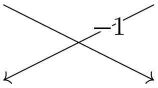
When writing formulæ, we must sometimes depart from the graphical notation, in which permutations are written top-to-bottom or left-to-right and thanks to their arrows there is no ambiguity in knowing in

---

5 Note that the side of the action changes! It is best to always use the appropriate side, so as to avoid inverses. Recall, however, that every left action can be converted into a right action by setting $f^g := {}^{g^{-1}}f$ and vice versa.

which order to compose the labels. We invariably let permutations act on the right on sets, and thus '$\sigma\tau$' means 'first σ, then τ'.

Exercise 1.1. In the wreath product $W = \{\pm 1\} \wr \mathrm{Sym}(2)$, consider the element

$h =$ 

Show by concatenating the diagram with itself that h has order exactly 4. The group W has order 8; which of the order-8 groups is it?

Let us consider a wreath product $W = H \wr_X G$. In writing elements $w, w' \in W$ algebraically, we may express them in the form $w = fg$ with $f\colon X \to H$ and $g \in G$, or in the form $w' = gf$. In both cases, the element g and the function f are unique, by definition of the semidirect product. The compositions $(fg)(f'g')$ and $(gf)(g'f')$ are, in all cases, computed using the relation

$$g \cdot f = {}^{g}f \cdot g,$$

namely

$$(fg)(f'g') = (f \cdot {}^{g}f')(gg') \text{ and } (gf)(g'f') = (gg')({}^{(g')^{-1}}f \cdot f'). \qquad (1.2)$$

Exercise 1.2. Let R be a ring, viewed as a group under addition, and let RG denote the group ring of G, on which G acts by right multiplication. Show that $R \wr G$ is isomorphic to $RG \rtimes G$. More generally, let X be a G-set; then RX is a G-module. Show that $R \wr_X G$ and $RX \rtimes G$ are isomorphic.

1.1. Actions

Assume now, moreover, that H acts from the right on a set Y. Then there are two natural sets on which $W = H \wr_X G$ acts:

- There is an action on $Y \times X$, given by $(y, x) \cdot fg = (yf(x), xg)$ for $(y, x) \in Y \times X$; it is called the *imprimitive* action;
- There is an action on Y^X, the set of functions $X \to Y$, given by $(\phi \cdot fg)(xg) = \phi(x)f(x)$ for $\phi\colon X \to Y$; it is called the *primitive* action.

Exercise 1.3. There are natural bijections between the sets $(Z \times Y) \times X = Z \times (Y \times X)$ and $(Z^Y)^X = Z^{Y \times X}$. Assume now that a group G acts on X, a group H acts on Y and a group I acts on Z. Show that the bijections above give isomorphisms between the groups $(I \wr_Y H) \wr_X G$ and $(I \wr_{Y \times X} (H \wr_X G))$ as permutation groups, both of $Z \times Y \times X$ and of $(Z^Y)^X$.